

Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector

Marisa Reddy Randazzo, Ph.D.
Michelle Keeney, Ph.D.
Eileen Kowalski
National Threat Assessment Center
United States Secret Service
Washington, DC

Dawn Cappelli
Andrew Moore
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

August 2004



CarnegieMellon
Software Engineering Institute

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE AUG 2004		2. REPORT TYPE		3. DATES COVERED 00-00-2004 to 00-00-2004	
4. TITLE AND SUBTITLE Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 25	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Insider Threat Study:
Illicit Cyber Activity
in the
Banking and Finance Sector

Marisa Reddy Randazzo, Ph.D.
Michelle M. Keeney, Ph.D.
Eileen F. Kowalski
National Threat Assessment Center
United States Secret Service

Dawn M. Cappelli
Andrew P. Moore
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University

INTRODUCTION

For several months, beginning in the fall of 1996, two credit union employees worked together to alter credit reports in exchange for financial payment. As part of their normal responsibilities, the employees were permitted to alter credit reports based on updated information the company received. However, the employees intentionally misused their authorized access to remove negative credit indicators and add fictitious indicators of positive credit to specific credit histories in exchange for money. The total amount of fraud loss from their activities exceeded \$215,000. The risk exposure to the credit union was incalculable.

From 1997 until his detection in early 2002, a foreign currency trader with an investment bank used a range of tactics, including changing data in various trading systems, so it appeared he was one of the bank's star producers. In actuality, he lost the bank over \$600 million.

In March 2002, a "logic bomb"¹ deleted 10 billion files in the computer systems of an international financial services company. The incident affected over 1300 of the company's servers throughout the United States. The company sustained losses of approximately \$3 million, the amount required to repair damage and reconstruct deleted files. Investigations by law enforcement professionals and computer forensic professionals revealed the logic bomb had been planted by a

¹ *logic bomb*: malicious code implanted on a target system and configured to execute after a designated period of time or on the occurrence of a specified system action.

disgruntled employee who had recently quit the company because of a dispute over the amount of his annual bonus.

These incidents were all committed by “insiders”: individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm. Efforts to estimate how often companies face attacks from within are difficult to make. Many believe that insider attacks are under-reported to law enforcement agencies or prosecutors. Companies may fear the negative publicity or increased liability that may arise as a result of the incidents. Or, they may believe that the harm suffered would not be sufficient to warrant criminal charges.

Statistics vary regarding the prevalence of cases perpetrated by insiders compared to those perpetrated by individuals external to the targeted organizations.² Nevertheless, insiders pose a substantial threat by virtue of their knowledge of and access to their employers’ systems and/or databases, and their ability to bypass existing physical and electronic security measures through legitimate means.

Previous efforts have been made to study insider incidents, including workshops to develop a foundation of knowledge on insider threats³; annual surveys of organizations on the number of insider incidents they have experienced in a given year⁴; and, in-depth case studies of information technology insiders.⁵ However, these studies have focused on convenience samples and more narrow areas of industry. Additionally, other efforts have not examined the incidents from both behavioral and technical perspectives simultaneously. These gaps in the literature have made it difficult for organizations to develop a more comprehensive understanding of the insider threat and address the issue from an approach that draws upon human resources, corporate security, and information security perspectives.

The Secret Service National Threat Assessment Center (NTAC) and the CERT Coordination Center of Carnegie Mellon University’s Software Engineering Institute (CERT/CC) joined efforts to conduct a unique study of insider incidents, the Insider Threat Study (ITS), examining each case from a behavioral and a technical perspective. This effort was made possible, in part, through funding by the Department of Homeland Security, Office of Science and Technology, which

² Richardson, R. (2003). Eighth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

³ Anderson, R.H. (1999, August). Research and Development Initiatives Focused on Prevention, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. Santa Monica, CA: RAND (CF151); Department of Defense (2000). DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team. Washington, DC: Author.

⁴ CSO Magazine, United States Secret Service and CERT® Coordination Center. (2004). 2004 eCrime Watch Survey. Framingham, MA: CXO Media; Richardson, R. (2003). Eighth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

⁵ Shaw, E., Post, J., and Ruby, K. (August 31, 1999). Final Report: Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations.

provided financial support for the study in fiscal years 2003 and 2004. Section 1 of this report presents an overview of the ITS, including its background, scope, and study methods. Section 2 reports the findings and implications specific to research conducted on insider threat in the banking and finance sector.

SECTION 1: INSIDER THREAT STUDY OVERVIEW

Background

Securing cyberspace has become a national priority. In *The National Strategy to Secure Cyberspace*⁶, the President's Critical Infrastructure Protection Board identified several critical infrastructure sectors:

- banking and finance
- information and telecommunications
- transportation
- postal and shipping
- emergency services
- continuity of government
- public health
- food
- energy
- water
- chemical industry and hazardous materials
- agriculture
- defense industrial base

The National Strategy to Secure Cyberspace emphasizes the importance of public-private partnerships in securing these critical infrastructures and improving national cyber security. Similarly, one focus of the Department of Homeland Security is enhancing protection for critical infrastructure and networks by promoting working relationships between the government and private industry. The federal government has acknowledged that these relations are vital because most of America's critical infrastructure is privately held.

Since 2001, the United States Secret Service (Secret Service) and CERT/CC have collaborated on multiple efforts to identify, assess, and manage potential threats to, and vulnerabilities of, data and critical systems. The collaboration represents an effort to augment security and protective practices through two components:

⁶ The National Strategy to Secure Cyberspace. (February 2003).
<http://www.whitehouse.gov/pcipb/>

1. Finding ways to identify, assess, and mitigate cyber security threats to data and critical systems that impact physical security or threaten the mission of the organization
2. Finding ways to identify, assess, and manage individuals who may pose a threat to those data or critical systems

The overall goal of the collaborative effort is to develop information and tools that can help private industry, government, and law enforcement identify cyber security issues that can impact physical or operational security and to assess potential threats to, and vulnerabilities in, data and critical systems. One component of this collaboration, the ITS, focuses on the *people* who have access to such information systems and have perpetrated harm using them. The project combines the Secret Service's expertise in behavioral and incident analysis with CERT/CC's technical expertise in network systems survivability and security.

The ITS is an extension of earlier studies conducted by both organizations. Two previous Secret Service studies, the Exceptional Case Study Project and the Safe School Initiative, focused on identifying information that was operationally relevant and that could help prevent future violent or disruptive incidents. The goal of this earlier research was to find information that could help enhance threat assessment efforts – efforts to identify, assess, and manage the risk of harm an individual may pose, before the individual has an opportunity to engage in violent behavior.

Previous CERT/CC research, sponsored by the Department of Defense, focused on cyber insider threats in the military services and defense agencies. The work is part of an ongoing partnership between CERT/CC and the Defense Personnel Security Research Center (PERSEREC) in response to recommendations in the 2000 *DoD Insider Threat Mitigation* report⁷. It will identify characteristics of the environment surrounding insider cyber events evaluated for criminal prosecution by DoD investigative services. The primary use of this information will be to guide future operating, security, and personnel procedures to reduce the threat to critical information systems in the DoD and its contractor community.

Insider Threat Study Scope

The goal of the overall ITS is to develop information to help private industry, government, and law enforcement better understand, detect, and ultimately prevent harmful insider activity. The study consists of several components:

- an aggregated case-study analysis that provides an in-depth look at insider incidents that have occurred in critical infrastructure sectors between 1996 and 2002 (this report presents the first findings from this analysis)

⁷ www.defenselink.mil/c3i/org/sio/iptreport4_26dbl.doc

- a review of the prevalence of insider activity across critical infrastructure sectors over a 10-year time frame
- a survey of recent insider activity experienced by a sample of public- and private-sector organizations⁸

This first report – from the aggregated case study analysis – examines insider incidents within the banking and finance sector. Subsequent reports from the aggregated case study analysis will examine insider activity within the information and telecommunications sector and government sector, as well as incidents across critical infrastructure sectors.

Study Method

Study Sample

The cases examined are incidents perpetrated by insiders (current or former employees or contractors) who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations. Incidents included any compromise, manipulation of, unauthorized access to, exceeding authorized access to, tampering with, or disabling of any information system, network, or data. The cases examined also included any in which there was an unauthorized or illegal attempt to view, disclose, retrieve, delete, change, or add information.

Cases were identified through public reporting or as a computer fraud case investigated by the Secret Service.⁹ Public reporting included references in various media outlets (found through searches on Lexis-Nexis news databases and Internet search engines such as Google) and criminal justice databases (found through searches on Lexis court databases).

The cases studied here may or may not be representative of cases not mentioned in media, court, or Secret Service databases. As noted, organizations may be reluctant to expose these incidents, even to law enforcement. This report and others from the study will articulate only what we found among these known cases, but can say nothing about cases not known or reported. This uncertainty limits the ability to generalize the study findings and underscores the difficulty other researchers have faced in trying to better understand the insider threat. To the extent that such incidents are not reported outside of the organization in which they occur, efforts to fully understand the prevalence of insider incidents – and subsequently to find ways to prevent them – will likely be similarly limited.

⁸ CSO Magazine, United States Secret Service and CERT® Coordination Center. (2004). 2004 eCrime Watch Survey. Framingham, MA: CXO Media.

⁹ Examples of computer fraud cases include cases where an individual(s) fraudulently obtains a credit card issuer's records via a computer; places a virus, Trojan horse, or worm on, or conducts a denial-of-service attack against a computer; or obtains unauthorized access to a computer system by using a password.

This limitation does not, however, diminish the value in analyzing these incidents. The fact remains that insiders *have* perpetrated illicit acts against organizations in the critical infrastructure sectors. Their acts have disrupted these organizations, inflicted significant financial loss, and tarnished corporate reputations that took years to establish. While limited, this study provides insight into actual criminal acts committed by insiders. We believe this insight may be useful to those in the sectors charged with protecting their critical assets as they begin to examine ways of improving their defense against insider attacks.

Once CERT/CC and Secret Service researchers identified the cases, they categorized them according to the critical infrastructure sector of the affected organization. Some organizations fit into multiple critical infrastructure sectors (for instance, if the business of the organization was multi-faceted or crossed sector areas), but were included in the study under the primary business focus of the organization.

Procedure

The ITS adapted methods used in previous research performed by the Secret Service and CERT/CC to conduct in-depth examinations of network, system, and data compromises and other insider activity. Researchers focused primarily on tracing insider incidents from the initial harm backward in time to when the idea of committing the incident first occurred to the insider. In tracing the incidents backward, researchers tried to identify the behaviors and communications in which the insiders engaged – both online and offline – prior to and including the insiders' harmful activities.

For each case examined in the study, researchers from the Secret Service and from CERT/CC answered several hundred questions about the insider and the behavioral and technical aspects of the incident. The questions were organized around the following major topic areas:

1. components of the incident
2. detection of the incident and identification of the insider
3. pre-incident planning and communication
4. nature of harm to the organization
5. law enforcement and organizational response
6. characteristics of the insider and the organization
7. insider background and history
8. insider technical expertise and interests

For each case, Secret Service and CERT/CC researchers reviewed primary source material on the case, including investigative reports, court records, news articles, and other materials.¹⁰ Researchers also conducted supplemental interviews with case investigators and organization representatives.¹¹

SECTION 2: INSIDER ACTIVITY IN THE BANKING AND FINANCE SECTOR

This report examines **23 incidents** carried out by **26 insiders** in the banking and finance sector between 1996 and 2002. Organizations affected by insider activity in this sector include credit unions, banks, investment firms, credit bureaus, and other companies whose activities fall within this sector. Of the 23 incidents, 15 involved fraud, four involved theft of intellectual property, and four involved sabotage to the information system/network. Appendix A provides tables on the number of incidents by year, state, and organization size.

Findings and Implications

The following information represents the major findings observed across the insiders and incidents studied in the banking and finance sector.

Finding 1: Most Incidents Required Little Technical Sophistication

Most of the incidents examined in the banking and finance sector were not technically sophisticated or complex. That is, they typically involved exploitation of non-technical vulnerabilities such as business rules or organization policies (rather than vulnerabilities in an information system or network) and were carried out by individuals who had little or no technical expertise.

- In 87% of the cases studied, the insiders employed simple, legitimate user commands to carry out the incidents. In only a small number of cases was a more technical knowledge of network security required. For example, very few cases were carried out via a script or program¹² (9%), and only slightly more involved spoofing¹³ or flooding¹⁴ (13%).

¹⁰ Appendix B provides a list of Secret Service and CERT/CC personnel who reviewed cases for the study.

¹¹ For the banking and finance sector report, researchers interviewed representatives from eight companies and 17 law enforcement and/or prosecutorial agencies, as well as two of the insiders whose incidents were reviewed for the study.

¹² Scripts or programs can be written to execute a series of commands against the operating system, application, data, or network. A few examples of scripts or programs are UNIX shell scripts, Trojan horse programs, or password-cracking programs.

¹³ *spoof*: a user assumes the appearance of a different entity in network communications.

¹⁴ *flood*: a user accesses a target repeatedly in order to overload the target's capacity.

There was no evidence that any insider scanned computer systems to discover vulnerabilities prior to the incident.

- In 70% of cases studied, the insiders exploited or attempted to exploit systemic vulnerabilities in applications and/or processes or procedures (e.g., business rule checks, authorized overrides) to carry out the incidents. In 61% of the cases, the insiders exploited vulnerabilities inherent in the design of the hardware, software, or network.
- In 78% of the incidents, the insiders were authorized users with active computer accounts at the time of the incident. In 43% of the cases, the insider used his or her own username and password to carry out the incident.¹⁵
- However, there were some cases in which the insider used other means beyond his or her user account to perpetrate the harm. Twenty-six percent of the cases involved the use of someone else's computer account, physical use of an unattended terminal with an open user account, or social engineering (i.e., gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data).¹⁶
- Only 23% of the insiders were employed in technical positions¹⁷, with 17% of the insiders possessing system administrator/root access within the organization.
- Thirty-nine percent of the insiders were unaware of the organizations' technical security measures.¹⁸

Implications

Most incidents in the banking and finance sector report required minimal technical skill to carry out and were perpetrated by non-technical personnel with little computer knowledge or training. This suggests it is important for organizations to secure their networks from the full range of users, from persons responsible for data entry to management to system administrators. Also, many

¹⁵ Data were only available for 18 of the 23 incidents studied. The percentage of known data is 56% (10/18).

¹⁶ Data were only available for 18 of the 23 incidents studied. The percentage of known data is 33% (6/18).

¹⁷ A technical position is one requiring specialized skills in information technology, such as programming, scripting, networking, information security, or system architecture and configuration.

¹⁸ Data were only available for 20 of the 26 insiders studied. The percentage of known data is 50% (10/20).

of the cases involved the exploitation of inadequate or non-existent practices, policies, and procedures, including both those addressing technical practices and non-technical ones.

In one case, an insider who worked for a credit card point-of-sale terminal vendor used social engineering to obtain authentication information from the credit card company help staff. The insider posed as a distraught individual (with a fabricated identity) working for a particular, authorized merchant needing help with a malfunctioning terminal. He was then able to credit his own credit card by reprogramming a terminal using the information he had obtained. Reducing the risk of these types of technically unsophisticated attacks may require organizations to look beyond their information technology to their overall business processes, and the interplay between those processes and the technologies used.

Although most of the cases involved little technical skill, there were some cases in which significant technical knowledge of network security or the organization's information systems was required to carry out the incident. This finding suggests an additional need for techniques that monitor for more sophisticated network activities that may indicate a potential for harm. In fact, the four cases involving sabotage to the system or network were perpetrated by the only four insiders who were employed in technical positions.

In one case, mentioned previously, the insider constructed a "logic bomb," distributed it remotely to hundreds of the company's servers across the country, and detonated it to delete programs critical to the business. The insider timed the logic bomb detonation to be most disruptive to the company's operations.

In another case, a currency trader (who also happened to have a college minor in computer science) developed much of the software used by his organization to record, manage, confirm, and audit trades. He wrote the software in a manner that allowed him to conceal his illegal trades, evolving the software over time to facilitate different methods of hiding his activities to reduce the risk of detection. In this case, it was nearly impossible for auditors to detect his activities. The insider, who consented to be interviewed for this study, told the study researchers that problems can arise when "the fox is guarding the henhouse." Specifically, the insider's supervisor managed both the insider's activities and the auditing department that was responsible for ensuring trades by the insider and his colleagues were legal or compliant.

When auditing department personnel raised concern about the insider's activities, they were doing so to the insider's supervisor (who happened to be their supervisor as well). The direction auditing department personnel received was not to worry about the insider's activities and to cease raising concern, for fear the insider would become frustrated and quit. Segregation of duties can help ensure that end-users of key financial systems cannot modify the system, or access the underlying data directly.

The insider also stated that group trading (trading by a team of traders), rather than individual trading, can help mitigate an organization's risks by making it easier to detect illegal or suspicious trading practices because there are multiple team members trading from the same account.

In some cases, the insider used means beyond his or her user account to perpetrate the harm. For example, some of the incidents were enabled by poor password and account management practices. In one case, an organization assigned default employee passwords that were widely known to be the employee's office number. In other cases, passwords were explicitly shared among multiple users. Poor password management makes identification of the insider much more difficult, because no one can be sure that activity associated with one employee's computer account is really the activity of that employee.

Proactive practices, such as mandatory password protection and change policies, and use of password-protected screen savers, can minimize the possibility of insiders using another employee's computer and/or account to carry out the attack. Computer accounts, system authorizations, and remote access should also be deactivated immediately when employment, consulting, or contracting agreements are terminated for any reason.

One insider employed at a credit union, who had system administrator access, was terminated and his account disabled. However, the credit union neglected to disable his remote access to the organization's network through the firewall. Company personnel also failed to change the root password. These oversights enabled the insider to sabotage the system, making it inaccessible for three days. If his remote access had been terminated, his actions may have been prevented.

Finding 2: Perpetrators Planned Their Actions

Most of the incidents were thought out and planned in advance. In most cases, others had knowledge of the insider's intentions, plans, and/or activities. Those who knew were often directly involved in the planning or stood to benefit from the activity.

- In 81% of the incidents, the insiders planned their actions in advance.
- In 85% of the incidents, someone other than the insider had full or partial knowledge about the insider's intentions, plans, and/or activities. These included
 - individuals involved in the incident and/or potential beneficiaries of the insider activity (74%)
 - co-workers (22%)
 - friends (13%)
 - family members (9%)

- In 61% of the cases, individuals from more than one area of the insider's life knew something of the insider's intentions, plans, and/or ongoing activities.
- In 31% of the incidents, there was some indication that the insider's planning behavior was noticeable. Planning behaviors included stealing administrative level passwords, copying information from a home computer onto the organization's system, and approaching a former coworker for help in changing financial data.
- In 35% of the incidents, the insider engaged in preparatory, incident-related behaviors. These behaviors included
 - planning discussions with competitors
 - planning discussions with co-conspirators
 - construction of a logic bomb on the organization's network
- Sixty-five percent of the insiders did not consider the possible negative consequences associated with carrying out the incident.

Implications

The fact that most of the incidents were planned in advance and that others had knowledge of the insiders' intentions, plans, and/or ongoing activities suggests that some future incidents may be prevented and/or detected at an earlier date. Law enforcement professionals, corporate security personnel, and other investigators may be able to uncover information about an insider's plan or find evidence of planning, preparations, or ongoing activity. The same may be true for line supervisors and others who may be in a position to observe or learn of an insider's behavior. Both security personnel and those outside the typical security chain can make a difference and help stop an insider before an incident occurs or before further damage can be done.

Investigators may be able to gather information about an insider and his or her intentions from a variety of sources: co-workers, family members, friends, as well as those potentially involved in the planned activity. Questions about others who may be involved with the insider or who may benefit from the insider's activities could point to those who have some information about the insider's intention or incident-related behavior.

Organizations can also explore ways to allow employees to report suspicious behavior to one central person or location. Attempts to get coworkers to share passwords, attempts to create unnecessary shared accounts, attempts to gain authorized access to accounts beyond the scope of an employee's job responsibilities, attempts to bypass technical safeguards, and disregarding acceptable use policies are all examples of behavior that would warrant further

inquiry. By encouraging employees to alert security personnel or others to behavior that appears incongruous with regular workplace activities, security personnel may have an opportunity to inquire about potential harmful activity and possibly intervene before it becomes a problem for the organization.

In spite of the attention they devoted to planning their illicit activities, many of the insiders were not aware of the potential negative consequences associated with carrying them out. Thus, efforts to increase an employee's awareness of the organization's ability to monitor activities and of the possibility of a prosecution or civil lawsuit against the insider (such as through the use of security banners on employees' computers) may be an important addition to an organization's practices for prevention.

One insider interviewed for the study commented that he did not foresee the magnitude of the consequences of his actions. He noted that as a result of his incident, he cannot pass a background check, is concerned about his potential for future employment, and said that the top result in a search for his full name on Google returns information on the incident. He expressed his belief that had he known of and considered these repercussions, he would not have entered the company's system following his employment termination.

Finding 3: Financial Gain Motivated Most Perpetrators

Most insiders were motivated by financial gain, rather than a desire to harm the company or information system. Other motives included revenge, dissatisfaction with company management, culture or policies, and a desire for respect.

- The motive and goal¹⁹ for most insiders studied was the prospect of financial gain (both 81%). Twenty-seven percent of the insiders studied were experiencing financial difficulty at the time of the incident.²⁰
- Beyond financial gain, insiders had other motives and goals. Some insiders were motivated by
 - revenge (23%)
 - dissatisfaction with the company management, culture, or policies (15%)
 - a desire for respect (15%)

¹⁹ For each insider, researchers coded both the insider's motive (the reason or reasons *why* the insider engaged in the incident; for example, revenge) and the insider's goal (*what* the insider was trying to accomplish with the incident; for example, destroying the company's reputation).

²⁰ Data were only available for 18 of the 26 insiders studied. The percentage of known insiders is 39% (7/18).

- Similarly, insiders had goals other than financial gain. Twenty-seven percent of the insiders deliberately tried to sabotage the business operations, data, or the organization's information system/network. Some of the insiders also set out to steal proprietary information (19%).
- In 27% of the incidents, insiders had multiple motives for engaging in the incident.

Implications

Financial gain was the most prevalent motive and goal among the incidents examined in the banking and finance sector report. Although many insiders in this sector damaged a system or data to accomplish their activities, their actions were in pursuit of a financial goal, rather than malicious intent to harm the system. In many of the cases, the harm to data was caused by someone altering a record to receive a check or improve a credit report. In a case mentioned previously, a foreign exchange trader “fixed” bank records to make his trading losses look like major gains for the bank in order to keep his job. In doing so, he managed to obtain lucrative bonuses for several successive years. In several cases, outsiders paid authorized users to improperly modify data.

Although financial gain influenced the motive and goal of most insiders, there were a few cases in which the insiders' activities were conducted for other reasons. For example, an information systems specialist terminated from his position for (reportedly) non-performance issues logged into the system that evening and entered UNIX commands until the system shut down. He reported that he was upset at his former employer, knew of the vulnerabilities in the company's network, and wanted to disrupt the system to inconvenience his replacement in the middle of the night.

One insider interviewed as part of the study, who was also terminated from his position, stated that he wanted company personnel “to feel the shame [he] had to go home with that night.” He also expressed a desire to demonstrate to company management that they should not have ignored his suggestions regarding computer security. This example further highlights the importance of discontinuing system access to employees who have been terminated to impede activity motivated by revenge with a goal of sabotaging the network or causing other harm to the organization.

Finding 4: Perpetrators did not Share a Common Profile

A wide variety of individuals perpetrated insider incidents in the cases studied. Most of the insiders in the banking and finance sector did not hold a technical position within their organization, did not have a history of engaging in technical attacks or “hacking,” and were not necessarily perceived as problem employees.

- Insiders ranged from 18 to 59 years of age. Forty-two percent of the insiders were female. Insiders came from a variety of racial and ethnic backgrounds, and were in a range of family situations, with 54% single and 31% married.
- Insiders were employed in a variety of positions within their organizations, including
 - service (31%)
 - administrative/clerical (23%)
 - professional (19%)
 - technical (23%)
- As reported earlier, only 17% of the insiders had system administrator/root access prior to the incident.
- Few of the insiders were known to be considered by management or co-workers as difficult to manage (15%) or untrustworthy (4%). Among those insiders who held technical positions within the organization, 33% were perceived by management as difficult employees to manage.
- Nineteen percent of the insiders were perceived by others as disgruntled employees.²¹
- Twenty-seven percent of insiders had come to the attention of either a supervisor and/or coworker for some concerning behavior prior to the incident.²² Examples of these behaviors include increasing complaints to supervisors regarding salary dissatisfaction, increased cell phone use at the office, refusal to work with new supervisors, increased outbursts directed at coworkers, and isolation from coworkers.

²¹ Data were only available for 16 of the 26 insiders studied. The percentage of known cases is 56% (9/16).

²² Data were only available for 18 of the 26 insiders studied. The percentage of known cases is 39% (7/18).

- In 9% of the incidents, the insiders had a known history of electronic abuses or violations.²³ In only 13% of the cases was there evidence that the insider showed an interest in, possessed materials on, or engaged in “hacking.”
- Twenty-seven percent of the insiders had prior arrests.

Implications

Employees who committed insider crimes in the banking and finance sector in this study did not fit some previous characterizations of critical information technology insiders.²⁴ In the cases examined in this study, neither privileged access nor technical position were necessary conditions for those likely to engage in insider attacks. In fact, most insiders in the sector did not hold a technical position within the organization.

Most of the insiders were not known to be difficult to manage as employees, even less so among non-technical than technical insiders. One insider, who was viewed as a valued employee by both co-workers and management, committed credit card fraud after 10 years of outstanding service in the banking field. At the time of the incident, the insider was both well-paid and well-respected as a top salesman for the territory he managed. Management must be aware that common perceptions about who is likely to be an insider threat may be inaccurate.

The fact that over one quarter of the insiders had a criminal record prior to their incidents underscores the importance of looking into employee backgrounds prior to hiring. Background checks for prospective, and current, employees that include at least basic criminal history checks may help identify employees with histories of fraud, theft, or other criminal behavior.

²³ Data were only available for 13 of the 23 cases studied. The percentage of known cases is 15% (2/13).

²⁴ Shaw, E., Ruby, K.G., and Post, J.M. (1998). *Insider Threats to Critical Information Systems*, Technical Report #2: Characteristics of the Vulnerable Critical Information Technology Insider (CITI). Bethesda, MD: Political Psychology Associates, Ltd. Shaw, E., Post, J.M., and Ruby, K.G. (1999, December). *The Mind of the Insider*. Bethesda, MD: Political Psychology Associates, Ltd.

Finding 5: Incidents were Detected by Various Methods and People

Insider incidents were detected by a range of people (both internal to the organization and external), not just by security staff. Both manual and automated procedures played a role in detection.

- In 61% of the cases, the insiders were detected by persons who were not responsible for security, including
 - customers (35%)
 - supervisors (13%)
 - other non-security personnel (13%)²⁵
- Those who were detected by security staff were detected by a range of security professionals, including
 - corporate security department staff (4%)
 - information technology (IT) security staff or system administrators (13%)
 - staff responsible for information systems/data (17%)
- In at least 61% of the cases, insiders were caught through manual (i.e., non-automated) procedures, including an inability to log in, customer complaints, manual account audits, and notification by outsiders.²⁶
- Twenty-six percent of the insiders were caught through system failure or irregularities.
- In 22% of the cases, insiders were caught by auditing or monitoring procedures.
- In 74% of the cases, after detection, the insiders' identities were obtained using system logs.²⁷ In 30% of cases, forensic examination of the targeted network, system, or data or of the insider's home or work equipment helped to identify the insider as the one who committed the harmful behavior.

Implications

Little consistency was found in either who detected the incidents or how the insiders were detected. Incidents were detected by customers, security personnel, and non-security personnel. Customers detected at least 35% of the

²⁵ Note that in some cases the insiders were detected by multiple people.

²⁶ Data were only available for 16 of the 23 incidents studied. The percentage of known cases is 88% (14/16).

²⁷ Data were only available for 18 of the 23 incidents studied. The percentage of known cases is 94% (17/18).

insider incidents in this sector. These cases involved a range of customers from checking account holders who depend on the authentication of transactions, to credit card holders who depend on the confidentiality of their card numbers, to money lenders who depend on the integrity of the nation's credit history databases.

Further, with comparable rates of detection by non-security personnel and security personnel, an environment in which all employees are given responsibility for security awareness is important. Training managers and all staff on the business and security policies of the organization, as well as the repercussions for violating them, may enhance the organization's overall vigilance to insider activities. It is important for employees to understand that preventing or limiting damage due to insider activity benefits not only the organization but also the employees.

A formal process for employees to report suspected abuses is likewise integral to an effective security awareness policy. Employees must know how to report activity that raises concern. Increasing security awareness and responsibility among individual employees may further deter insider activities.

Most of the incidents were detected through manual (non-automated) procedures, which may have resulted in part from the low-level technical nature of the incidents. The non-technical nature of insider activity in the banking and finance sector implies that effective means of detection should also include non-technical measures. Incidents that depend only on simple, legitimate user commands executed using the insider's own computer account (characteristics of most of the cases in this study) are not events designed to be detected by most intrusion detection tools. Some inappropriate actions can be detected by automated checks in information systems. However, an older legacy system used in at least one case in this study did not implement automated checks, thresholds, or warnings.

Anomaly detection tools that monitor individual applications for user activity that deviates significantly from a pre-defined profile may be useful. However, these tools are known to be expensive to operate, only minimally effective, and not widely available. Therefore, it is likely that the detection and assessment of this class of insider incidents will continue to require manual diagnosis and analysis for the foreseeable future. As a result, near-term mitigation and effective countermeasures will come in the form of improved practices, policies, and procedures.

Auditing and monitoring procedures detected more than 20% of insider incidents in the banking and finance sector. These procedures included review of the audit logs, monitoring and observation of employee activity after a suspicious transaction, funds transfer review, auditing for fraudulent charges, and internal audits.

In one case, a loss prevention administrator detected suspicious credit card transactions and traced them back to the fraudulent activity of a credit card account manager. The account manager had changed the address associated with an account he managed, ordered a new credit card and PIN to be sent to his address, and withdrew money from an ATM using the card. Even though the insider tried to hide his crime by restoring the account information, the audit logs provided evidence of his criminal activity.

A note of caution: One insider interviewed for this report stated that, with respect to times when accounts were most likely to be audited, he knew “the end of the month was hot, the end of the quarter was hotter, and the end of the year was really hot.” As a result, he timed his illegal activity to avoid these periods of likely auditing. If auditing procedures are well-known, including the times they are typically conducted, insiders might be able to work around them to commit harmful activity.

In addition to system and network logs, application-level logging provides more detailed information regarding data access, modifications, and deletions to facilitate auditing and monitoring functions. If possible, all data access (read, modify, and delete) should be logged for individual data items in the organization's databases. At a minimum, the computer account, IP address, action taken, and time that action was performed should be logged, as these data can assist in the detection of insider attacks. It is important to back up these logs so they can be recovered, along with the application data. In addition, a procedure for periodic review of all logs is essential in a proactive monitoring process.

Although the insider attacks reported were primarily non-technical, technical means may be effective in identifying the insider once the attack itself is detected. To perform this identification, organizations without a technical security department (or system administrators trained in forensics) may benefit from outsourcing investigations to external security organizations or law enforcement.

Finding 6: Victim Organizations Suffered Financial Loss

The impact of nearly all insider incidents in the banking and finance sector was financial loss for the victim organization. Many victim organizations incurred harm to multiple aspects of the organization.

- Nearly all of the organizations experienced financial loss as a result of the insiders' actions (91%). Losses ranged from a low of \$168.00 to over \$691 million. In 30% of the cases, the financial loss was in excess of \$500,000. One company did not suffer any financial loss.
- In 91% of the cases, the insider activity had at least one other adverse impact on the organization.

- Other harm incurred by the organizations included damage to business operations (30%) and to the organization's reputation (26%).
- In addition, all of the cases involved attacks that affected the security of the organizations' data, while only 22% involved attacks that affected the security of the organizations' information systems/networks. Only 9% of the cases involved insiders that targeted an organization's network, components, or external connectivity.
- There was no adverse impact to facilities, personnel security, national security, or harm to specific individuals.
- Seventy-eight percent of the cases involved the modification and/or deletion of information.

Implications

By virtue of their industry focus, organizations in the banking and finance sector must provide direct access to financial resources to many of their employees, from bank tellers to system administrators. As a result, there are opportunities for various technical and non-technical employees, using legitimate commands and their own computer accounts, to harm the data of the organization. In this sector, harm to the integrity of an organization's data typically coincided with major financial loss that resulted from insiders motivated by financial gain.

In addition, financial loss caused by insider activity may harm an organization's reputation. In one case referenced earlier, in which a foreign currency trader modified bank records to make his trading losses look like trading gains over a five-year period, the resulting liabilities for the bank drew a large amount of media attention. In another case, an insider purchased "put" options (a type of security that increases in value when the organization's stock price declines) for the organization's stock prior to planting a logic bomb within the organization's network. It appears that the insider was betting the organization's stock price would plummet once word got out that the logic bomb had deleted billions of the organization's files, and that he would stand to make a considerable financial profit as a result.

Improper data modifications in some cases further resulted in the issuing of loans to unqualified individuals, loss of funds, and harm to organizational reputations, all of which equals increased risk exposure for the institution. Negative publicity about cases such as these could seriously impact the reputation and perceived trust of the institution.

Finding 7: Perpetrators Committed Acts While on the Job

Most of the incidents were executed at the workplace and during normal business hours.

- Eighty-three percent of the insider threat cases involved attacks that took place physically from within the insider's organization. In 70% of the cases, the incidents took place during normal working hours.
- Thirty percent of the incidents were carried out from the insiders' homes through remote access. Of those attacks, 57% involved actions both at the workplace and from home.

Implications

The fact that many of the insider attacks reviewed in this study took place at the office during normal working hours suggests that insider risk may be reduced by educating the workforce about how to prevent certain avenues of attack and how to respond to and report on suspicious behavior by co-workers. Examples include attempts to use someone else's computer, attempts to download or copy company information to a personal or home computer, and increasing combativeness with supervisors and/or coworkers.

Because some incidents involved the use of remote access to carry out the incident, caution is advised when an organization provides remote access to *critical* data, processes, or information systems. One insider interviewed for this study stated that it was easier to conduct his illicit activities from home because he did not have to worry about anyone looking over his shoulder.

To address this vulnerability, organizations could employ a layered security approach to allow remote access to email and non-critical data, but restrict access to critical data and information systems only to employees physically located inside the workplace. In one reported case, the insider changed the passwords to his previous employer's master account remotely from his residence two weeks after his resignation due to an internal dispute.

Similar to earlier recommendations, when remote access to critical data, processes, and information systems is deemed necessary, the organization should offset the added risk with closer logging and frequent auditing of remote transactions. Information such as login account, date/time connected and disconnected, and IP address should be logged for all remote logins. It also is useful to monitor failed remote logins, including the reason the login failed. If authorization for remote access to critical data is kept to a minimum, then it should be possible to assign responsibility for reviewing these logs on a daily basis.

Discussion

A key finding in this study is that insider attacks on organizations in the banking and finance sector required minimal technical skill to execute. Many of the cases involved the simple exploitation of inadequate practices, policies, or procedures. The insider threat activity examined in the banking and finance sector appears to involve an interaction among organizational culture, business practices, policies, and technology, as well as the insiders' motivations and external influences.

Reducing the risk of these attacks requires organizations to look beyond their information technology and security to their overall business processes. They must also examine the interplay between those processes and the technologies used. Management attention on financial performance, to the exclusion of good risk management practices, seems to be a recurrent theme in some of the cases in this study.

As mentioned earlier, one insider interviewed for the study mentioned that he had repeatedly informed management of the need for improved security on the company's systems and networks, but his warnings went unheeded. He said that management did not listen to him because of the cost of implementing improved security. Following his termination, he was able to exploit these security vulnerabilities to shut down the network. Better understanding of technical and operational risks may allow organizations in the banking and finance sector to make more informed decisions regarding the often complex tradeoffs between performance, security, and compliance. Comprehensive efforts to identify an organization's systemic vulnerabilities can help inform mitigation strategies for insider attacks at varying levels of technical sophistication.

Another important finding suggests that organizations in the sector cannot assume that only certain groups or classifications of employees within their organizations may pose potential threats. The insiders involved in the cases studied did not share a common profile, were not necessarily problem employees, and showed considerable variability in their range of technical knowledge.

Financial gain was clearly the most prevalent motive and goal in these cases. By virtue of the services they provide, organizations within this sector must provide direct access to financial resources to many of its employees, from bank tellers to system administrators. Since most incidents included in this study required minimal technical skill to carry out, there are opportunities for both technical and non-technical employees in various positions in banking and finance organizations to cause significant damage, financially, legally, and to the reputation of the organization. The findings from this study suggest that a wide variety of employees have carried out serious attacks targeting the financial assets of their organizations.

Since many of the insider attacks reviewed in this study took place at the office during normal working hours, it may help to train all staff with the goal of creating a culture of security in which suspicious or indicative behaviors are detected, monitored, reported, and investigated. Employees must know not only what to look for, but also how to report activity that raises concern. Such a culture can create self-reinforcing security in which insider activity is more likely to be detected before major damage is done, and can make employees think twice about engaging in the insider activity in the first place because of the increased awareness and monitoring. At the same time it would be counterproductive to create an environment of mistrust. It should be made clear that preventing or limiting the damage due to insider attacks is to the mutual benefit of the organization and its workforce.

Although questions asked about each case in this study included information on socio-environmental factors or stressors potentially related to the insider activity, there was insufficient information available from either investigative files or interviews with case investigators and organization supervisors to answer those questions. However, an interview with one insider suggested at least some role for socio-environmental factors: The sentiment on a sign hanging on the insider's office wall stated, "It's only money and it's not even ours." In addition, the anonymous nature of online activities may embolden individuals to perform acts they would not otherwise do. One insider interviewed for the study stated "Do you walk up to a car and just try to unlock it? No ... that's disrespectful. Online, it feels okay." Finding ways to counter these attitudes among employees may ultimately assist banking and finance sector organizations in combating the insider threat.

APPENDIX A

Banking and Finance Sector – Insider Incidents by Year of Initial Damage

YEAR	Number of Incidents
1996	4
1997	4
1998	2
1999	1
2000	2
2001	7
2002	3

Banking and Finance Sector – Locations of Insider Incidents by State

State	Number of Incidents
California	1
Florida	1
Illinois	3
Kansas	1
Maine	1
Minnesota	2
Missouri	1
Nevada	1
New Jersey	1
New York	3
Ohio	2
Pennsylvania	1
Tennessee	1
Texas	3
Wisconsin	1

Banking and Finance Sector – Size of Organizations

Number of Employees	Number of Incidents
1 – 100	5
101 – 500	2
501 – 3,000	4
3,001 – 10,000	5
10,001 – 50,000	1
Over 50,000	2

APPENDIX B

The Secret Service and CERT/CC appreciate the work and dedication of the following personnel, without whose efforts this study would not have been possible. With many thanks to the Insider Threat Study research staff:

U.S. Secret Service, National Threat Assessment Center

Brandi Justice
Diana McCauley
Eileen Kowalski
Georgeann Rooney
Jim McKinney
Lea Bauer
Lisa Eckl
Marisa Reddy Randazzo
Megan Williams
Michelle Keeney
Susan Keverline
Tara Conway

Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center

Andy Moore
Bill Wilson
Bradford Willke
Casey Dunlevy
Chris Bateman
Dave Iacovetti (USSS/CERT Liaison)
David Mundie
Dawn Cappelli
Mark Zajicek
Stephanie Rogers
Tim Shimeall
Tom Longstaff
Wayne Peterson (USSS/CERT Liaison)